Research Journal of Applied Sciences, Engineering and Technology 9(8): 583-593, 2015
DOI:10.19026/rjaset.9.1442
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2015 Maxwell Scientific Publication Corp.
Submitted: May 31, 2014 Accepted: November 26, 2014 Published: March 15, 2015

Research Article

Directional Advanced Intruder Handling Ad-hoc on Demand Distance Vector Protocol Using Divide and Conquer Strategy Implementation

[1]S. Hemalatha and [2]Paul Rodrigues
[1]Anna University,
[2]DMI College of Engineering, Chennai, Tamil Nadu, India

Abstract: The Aim of this study is to develop the protocol for identify the failure node, intruder node with power optimized routing protocol named Directional Advanced Intruder Handling Adhoc On demand Vector protocol. Mobile Ad-hoc Network is an infrastructure less network, nodes in mobile Ad-hoc are comprised to work with wireless nodes, can move freely and dynamically self organized in to arbitrary topologies. Over the past twenty years the development of Ad-hoc network was developed from tactical networks to Bluetooth, HyperLAN and IEEE 802.11. In the protocol stack of Ad-hoc network, the major issues on network layers, which has a responsibility to transfer the packets from one node to another. Many protocols have been proposed in Ad-hoc network, but none of the protocol is working under the principle of handling checking on packet delivery. This study presents the Directional Advanced Intruder Handling Ad-hoc on demand Vector protocol algorithm definition and implementation. The working principle of this protocol is checking the packet delivery to the destination. If any one of the nodes in the route is not forwarding the packet, that corresponding node will be identified and redirect the packet to the new route. For doing this checking this protocol uses divide and conquer strategy. The number hop between the source to destination is divided into two halves and check whether the up to the middle node the packet are flowing in a proper order or not. Recursively doing the divide and conquer of the route path, can identify the node which is not forward the packet to the next node. The design of this protocol itself able to identify the intruder in the routing path. Contains several stages from path discovery, packet transmits, apply divide and conquer strategy on route, identify the node which is not forward the packet, redirect the new path, alert all the nodes about the victim node. Finally performance of the protocol is improved with transmission in directional antennas.

Keywords: AAODV protocol, AD-HOC network, AODV protocol, divide and conquer

INTRODUCTION

A Collection of nodes formed a network under the working principles of move freely, organized themselves arbitrarily and without any administration is called Mobile Ad-hoc network (Wikipedia, 2004). In a common, a route between the source to destination through the Ad-hoc network is established by the routing protocol. The packets have followed this route to transfer the data. Packets are moved from a node to another node called the hop, until to reach the destination. A Routing protocol an Ad-hoc network is classified into two types is uniform protocol and non Uniform protocols. In uniform protocol each node sends and responds a routing control message. In non uniform type protocol reduces the number of nodes participating in routing computation (Murthy and Garcia-Luna-Aceves, 1994).

Routing protocols describe the state information into two ways like topology based protocol and destination based protocol (Kuosmanen, 2002; Stojmenovic and Wu, 2003; Murthy and Garcia-Luna-Aceves, 1994). The routing in topology based protocol each node makes a decision based on the topology information. This type based on link state protocol (Chiang *et al*., 1997; Jacquet *et al*., 1998). Routing in destination based protocol is maintaining a distance to a destination. A Routing protocol in an Ad-hoc network is divided into two main categories of proactive and reactive protocol. In proactive protocol nodes maintain routing information for all other nodes in the network is stored in a table is called a routing table. So this protocol is also named as a table driven protocol.

In the second type of protocol, route information is established when a packet transfers between the nodes. In the table driven protocol are Destination Sequence Distance Vector (DSDV) protocol (Perkins and Bhagwat, 1994), every node maintain a routing table of all other nodes is based on the shortest path from source to destination. When any topological changes occur in the network, the route table also changes. The maximum number of changes in maintain by a counter which is increment by one when any router table changed. Wireless Routing Protocol (WRP) is a

Corresponding Author: S. Hemalatha, Anna University, Chennai, Tamil Nadu, India

proactive protocol which maintains a four kind of table hold a detail like distance, link cost and route and message transmission information (Perkins and Royer, 1999). Clustered Gateway Switch Protocol is an extension of Destination Sequence Distance Vector routing protocol which includes clustering to increase the protocol scalability (Murthy and Garcia-Luna-Aceves, 1994). This protocol performance is improved by including methods like priority token scheduling, gateway code scheduling and path recursion. Optimization link state routing protocol (Chiang *et al*., 1997) optimized the multipoint relay. Each node identifies its multipoint relay, by flooding message to MRP will be received by the destination. Topology dissemination Based on Reverse Path Forwarding (TBRPF) (Bellur *et al*., 2001) is a link state routing with overhead reduction technology (Jacquet *et al*., 1998). Each node computes its shortest path tree to all other nodes, but to optimize bandwidth Fish Eye State routing Protocol (Bellur *et al*., 2001) is under the technique of Fish Eye state information about other nodes is based on how far away the defined nodes are. In source initiated routing protocols Dynamic Source Routing Protocol (Johnson and Maltz, 1996) each node maintains a route cache contain a route learned by the node. AODV (Perkins and Royer, 2000; Marti *et al*., 2000; Park and Corson, 1997, 1998; Abd Rahman and Zukarnain, 2009; Perkins *et al*., 2003) node create a route on demand to maintain a complete a route using DSDV algorithm. TORA (Giannoulis *et al*., 2007) is another source initiated on Demand protocol, in a concept of link reversal of direct Acyclic Graph. TORA has the capacity of routing repair. ABR routing protocol is on demand protocol route selection is based on the signal strength in the link.

The evolution of identifying intruder was started in the early 1987 onwards. In Dorothy (1987), Bace (1998, 2000) and Mukherjee *et al*. (1994), the computer abuse on real time intruder detection was proposed by dinning methods able to detect, break and penetration of intruder in the MANET (Marti *et al*., 2000; Yongguang and Wenke, 2000). Intruder was identified by proposed that watch dog and parthrater method was used to identify the node which do not able to forward the packet. This method also checks whether node forward the packet without modification or not. Second method used was knowledge based IDS paper, different attacker patterns are updated on the IDS. Any variations on the attacker patters are identified as a intruder. Third method used was sensor based. They used multiple sensor for collecting data from nodes, which is used to identify the intruder. Next method was a signature based intruder detection and Geo graphic zone based intrusion detection system. Next method was proposed an architecture is called cooperative intrusion detection architecture was used to detect intruders. This architecture forms a node hierarchy on the network, top level nodes in the network were responsible for identifying an intruder. In the year 2005 knowledge based IDS proposed who defined finite base machine through RIDAN architecture against the AODV routing process.

Directional antennas have a number of advantages over omni-directional antennas for ad hoc networking. By focusing energy only in the intended direction, directional antennas significantly increase the potential for spatial reuse. They provide a longer range and/or more stable links due to increased signal strength and reduced multipath components.

To best utilize directional antennas, a suitable Medium Access Control (MAC) protocol must be designed. Current MAC protocols, such as the IEEE 802.11 standard, do not benefit when using directional antennas, because these protocols have been designed for omnidirectional antennas. In this study, we present modified MAC protocols suitable for 802.11 based ad hoc networks using directional antennas. For instance, routing performance can be improved by using a directional antenna.

As a consequence, various research issues, including MAC, routing, transmission scheduling, location discovery and topology control, have been emerged to best utilize the benefit of using directional antennas.

Most of the current MAC protocols, such as IEEE 802.11 MAC standard, use a handshake mechanism implemented by exchanging small control frames named Request-to-Send (RTS) and Clear-to-Send (CTS).

The successful exchange of these two control frames reserves the channel for transmission of the, potentially longer, data frame and a short Acknowledgement (ACK) frame.

When using directional antennas, while one directional antenna at some node may be blocked other directional antennas at the same node may not be blocked, allowing transmission using the unblocked antennas. This property results in performance improvement when using directional antennas.

MATERIALS AND METHODS

DAIHAODV protocol design stages: This protocol implementation is divided into several stages are:

- Decide the path using AODV protocol select the threshold level battery power nodes
- Packet transmit
- Establish the divide and conquer strategy
- Identify the victim node and Intruder node
- Redirect the new route
- Sending alarm message to all the node

Figure 1 shows the flow of directional AIHAODV protocol, follows the above stages.

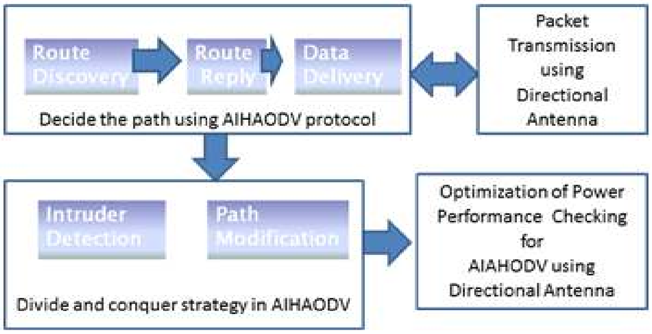
Route Discovery
Route Reply
Data Delivery
Decide the path using AIHAODV protocol
Packet Transmission using Directional Antenna
Intruder Detection
Path Modification
Divide and conquer strategy in AIHAODV
Optimization of Power Performance Checking for AIAHODV using Directional Antenna

Fig. 1: Stages of DAIHAODV protocol

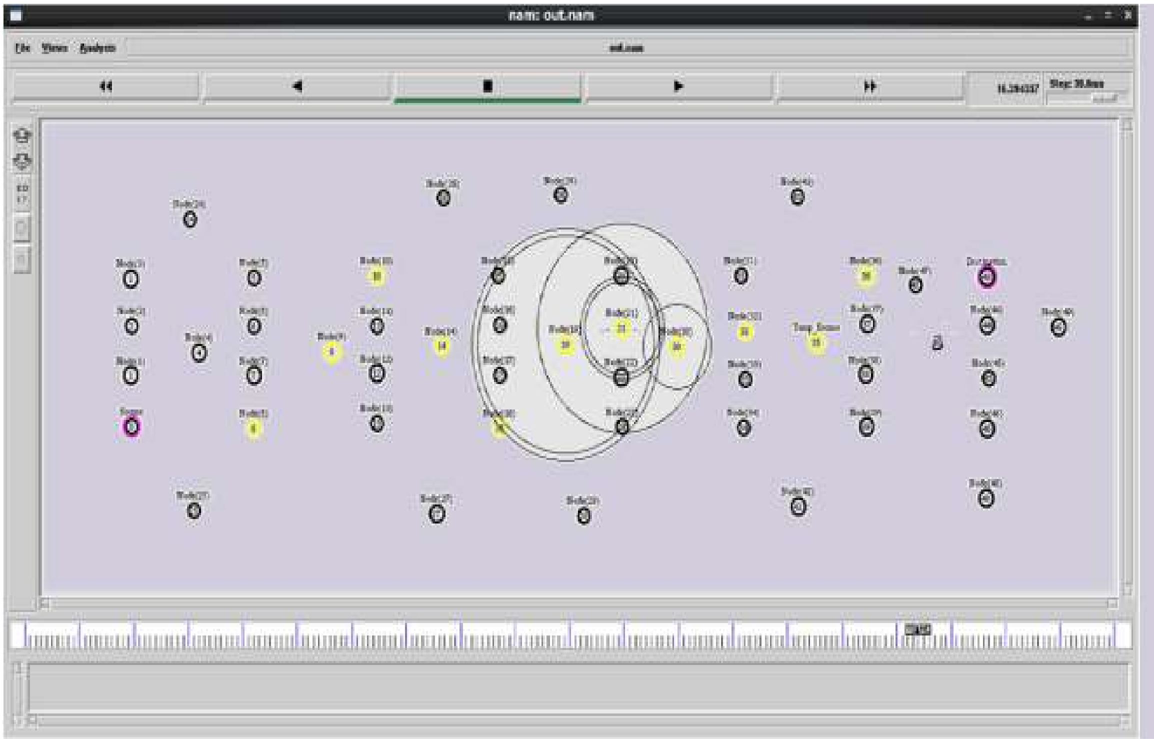

Fig. 2: Path identification based on threshold energy using AODV protocol

Decide the path using AODV protocol: Route discovery of this protocol will be based on Ad-hoc On Demand Vector protocol principle. Steps involved in Route Discovery:

- Node S (Source) needs a route to D (Destination)
- Creates a Route Request (RREQ): Enters D's IP addr, seq#, S's IP addr, seq#, hop count (= 0)
- Node S broadcasts aRREQ to neighbours
- Node A receives RREQ: Makes a reverse route entry for S dest = S, next hop = S, Hop count = 1 It has no routes to D, so it rebroadcasts RREQ
- Node C (intermediate node say C) receives RREQ: Makes a reverse route entry for S dest = S, nexthop = A, hopcount = 2 It has a route to D and the seq# for a route to D is > = D's seq# in RREQ

This module is processed with discover the route by using the AODV protocol as in Fig. 2 implemented in NS2. It can be done based on the route request and unicasting reply.

Packet transmit: Once the route between source to destination was identified, the packet is transferred from source to destination. This module is processed with packet transmission the packet can be transmitted via the route which is discovered by the AODV protocol as in Fig. 2. If the packet is reached properly to the destination, then the route is perfect and the route does not have any victim. If and packet loss or any delay occurred means it considers that the route have victimized. Identification purposes we are transmitting packet. Figure 3 Packet Transmit.

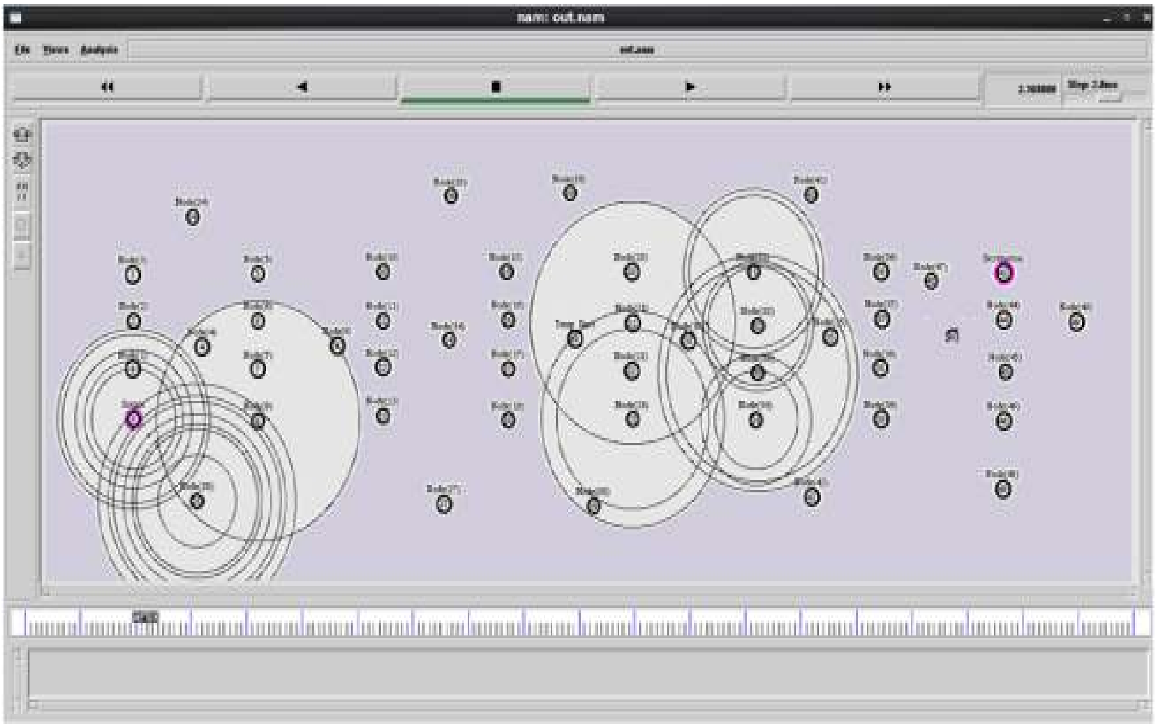

Fig. 3: Packet transmit

Establish the divide and conquer strategy: Customized protocol forwards the packet from source to identified destination. Then calculate the number of nodes and do the operation for giving divide and conquer strategy. In this strategy, the network can calculate the number of nodes and then it calculates the middle node, which the middle node will act as the temporary destination. Then the packet can be transmitted from the source to the temporary destination. If the temporary destination receives the packet then that node is not a victim. Then it will again calculate the number of remaining nodes. And find the middle node. That old middle node is acting as a temporary source and a new middle node will act as the temporary destination and do the process again. Else calculate the source node to middle node hop count and again do the new middle node and that will act as the temporary destination.

Divide and conquer strategy algorithm: Procedure (Source, Dest, G) -Divide and Conquer strategy
Consider the ordered Set G = {1……..N}

```
Step 1: Initialize source = 1, dest = N
Step 2: Calculate middle = No of hops (source to dest)
        /2
Step 3: (i) Check the packet is passed the middle node
        if yes the calculate the new middle form old
        middle (source = old middle) to dest, go to
        step 2
        (ii) otherwise calculate the new
        middle for source to middle (Dest = middle)
        (iii) repeat the process
        //assume there is no flow of data then suspect
        the node may be the intruder
        Process whether the middle node is intruder
        If True Set voctim = Middle and initiate route
        discovery process
Step 4: Process to conform victim node
Step 5: Process the flow of data in middle node
Step 6: If the flow is delayed, set Dest = prev (middle)
        and go to step 2
Step 7: If the flow is normal set source = next (middle)
        and go to step 2
Step 8: Stop
```

This module is processed with the strategy of divide and conquers; the packet can be transmitted via the route which is discovered by the AODV protocol as in Fig. 2. It can be calculate the number of nodes in the route as in Fig. 4. It can send the packet to the destination. If the packet is not reached to the destination, then the route is divided and middle node will act as the temporary destination as in Fig. 5. After a transmit ion that temporary destination receives the packet, then that node act as the temporary source as in Fig. 5.

Identify the victim node and intruder node: Using AIHAODV Routing protocol divide and conquer strategy can be done. Based on this strategy it can identify the victim node which does not forward the packet to the next node shown in Fig. 6.

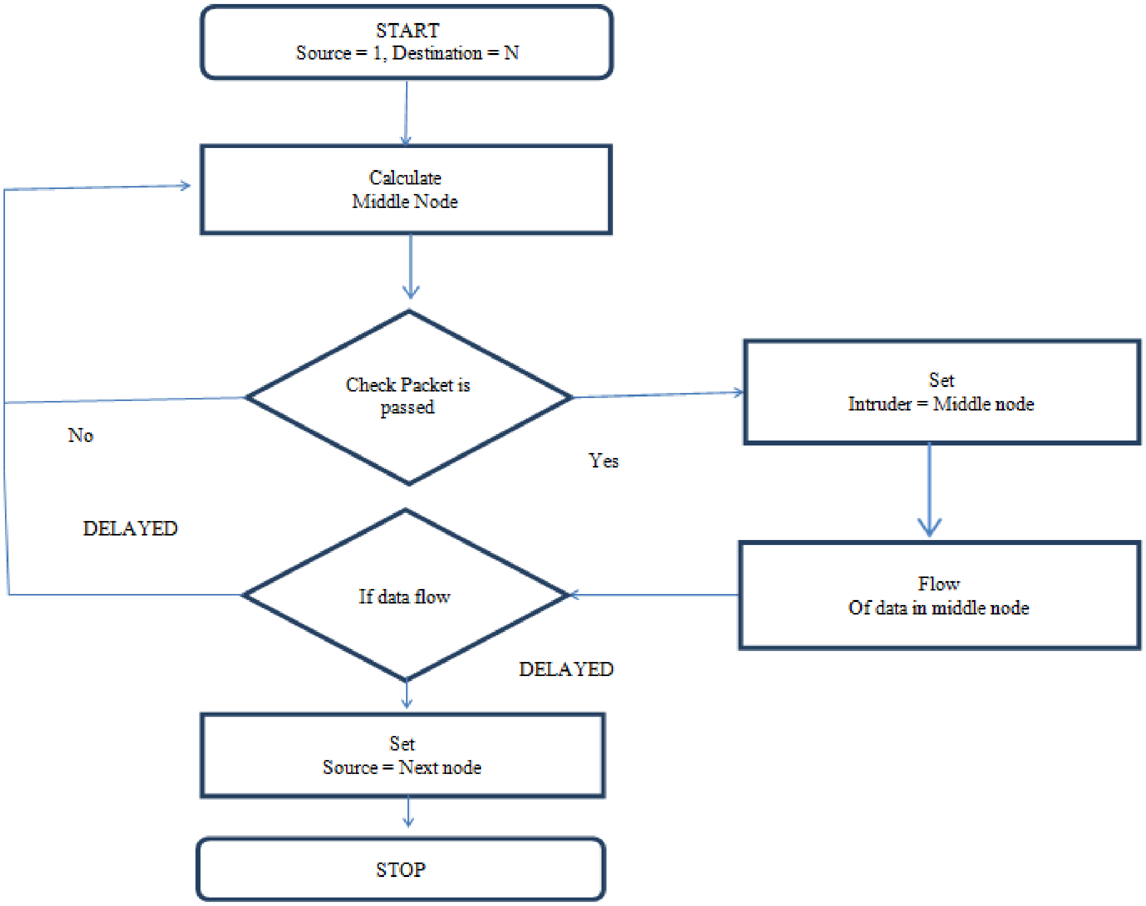

Fig. 4: Divide and conquer flow diagram

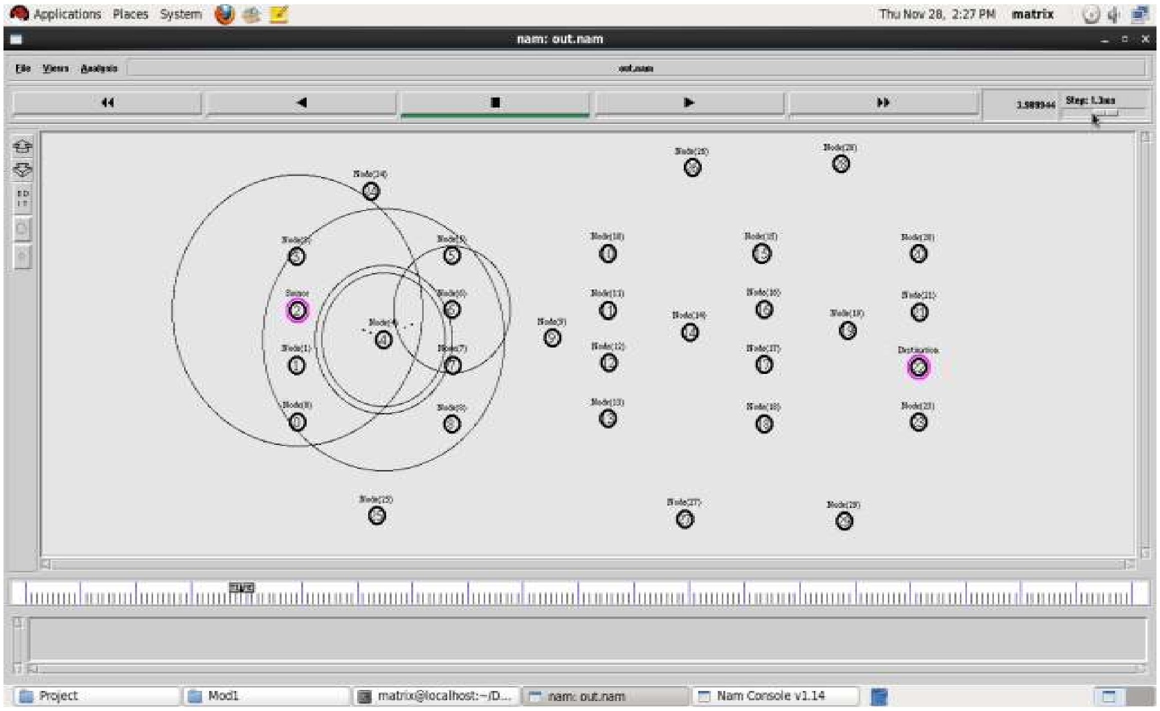

Fig. 5: Route discovery and number of node calculation

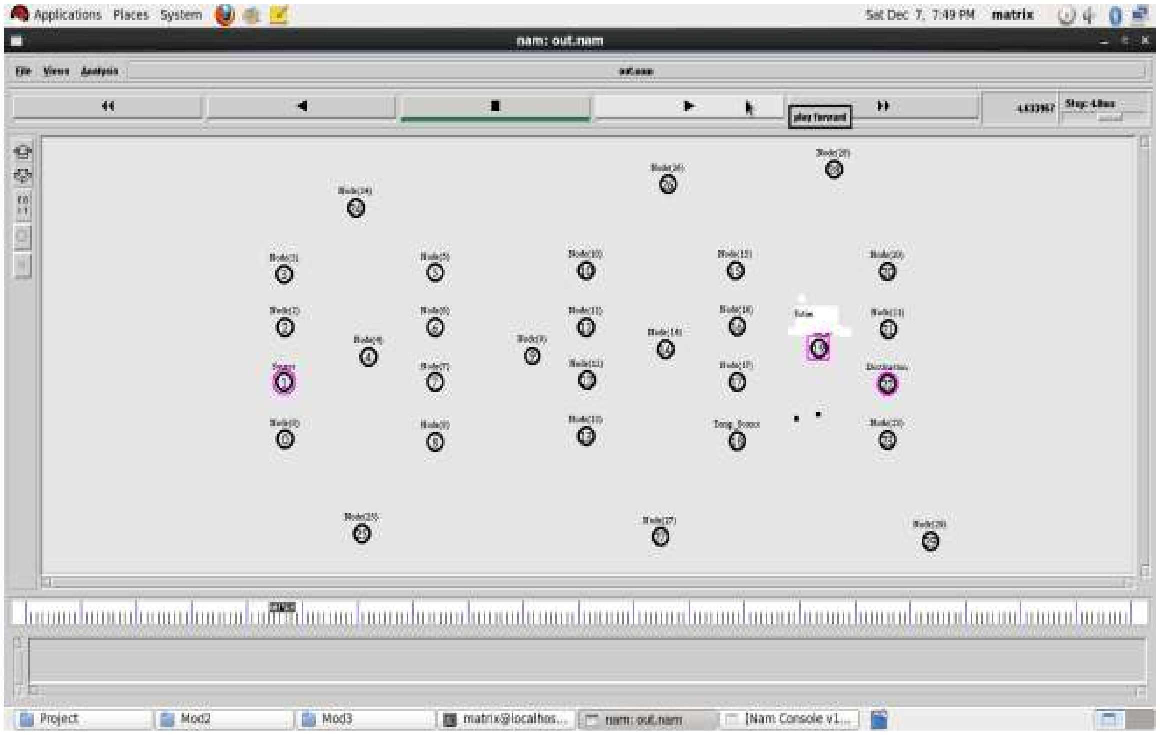

Fig. 6: Victim node identification

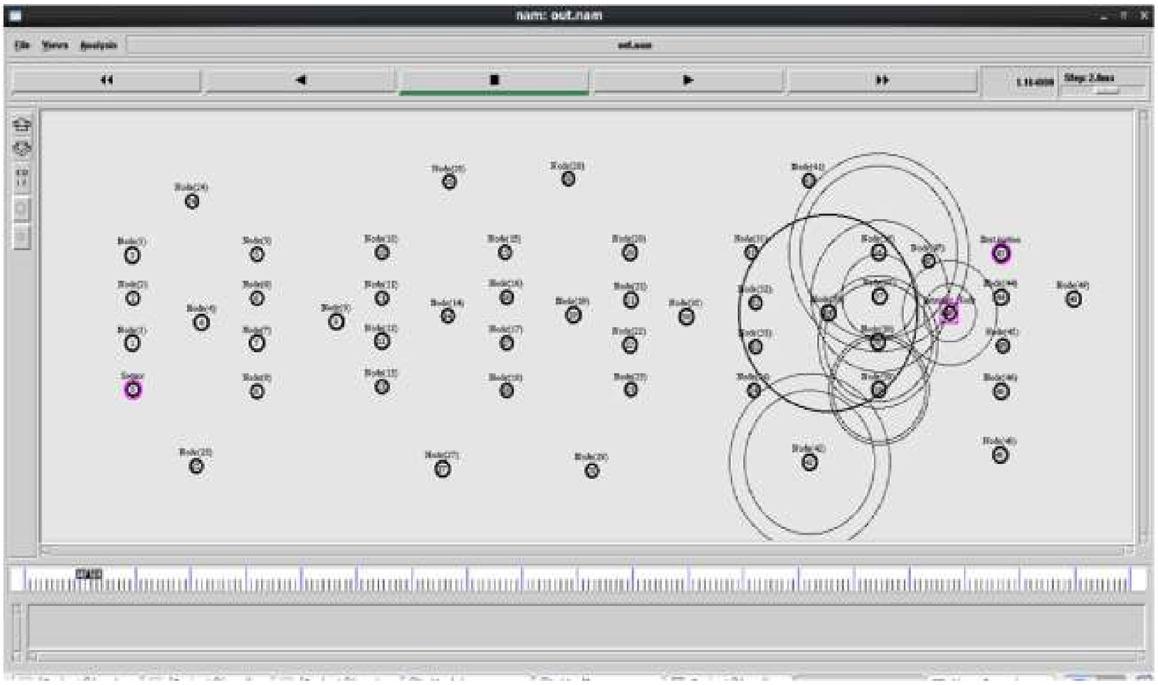

Fig. 7: Intruder node identification

For identification of intruder, protocol made the victim node as suspected node. Sends a route request to the suspected node, there is no reply comes from the node it is conformed as a intruder and send alert message about the intruder to all other node shown in Fig. 7.

Send alert message: This module is focused for sending alter the message to entire node after the victim node identified using divide and conquer strategy.

Route re-direction: This module is focused in the route redirection, after send an alert message it will

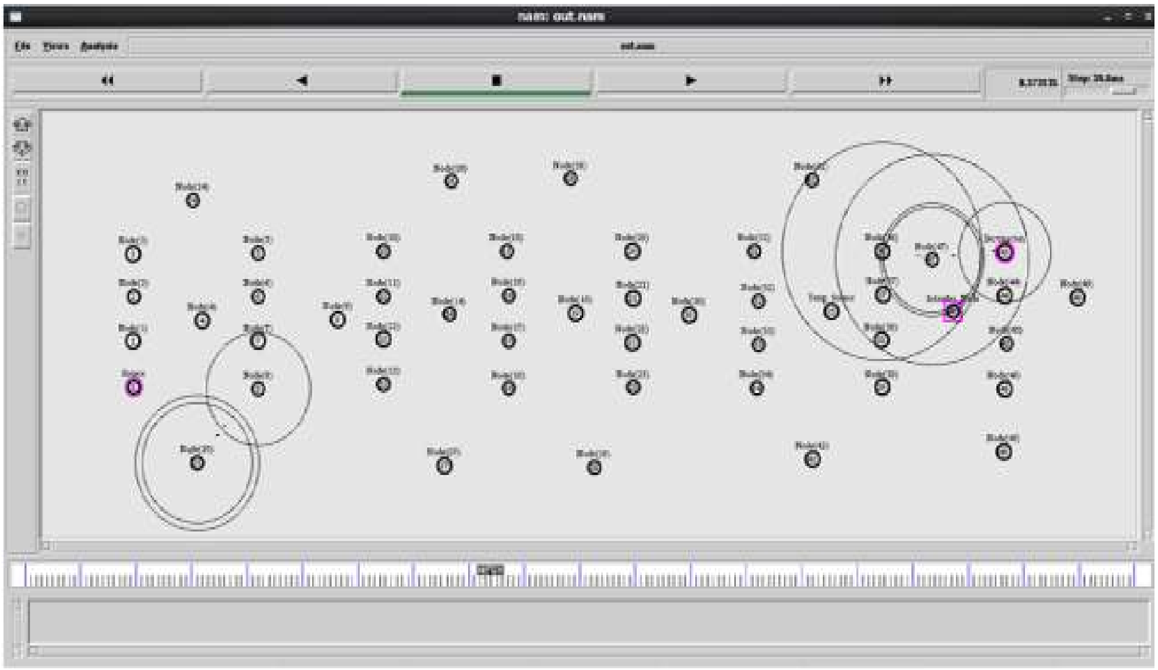

Fig. 8: Route re-direction initiation

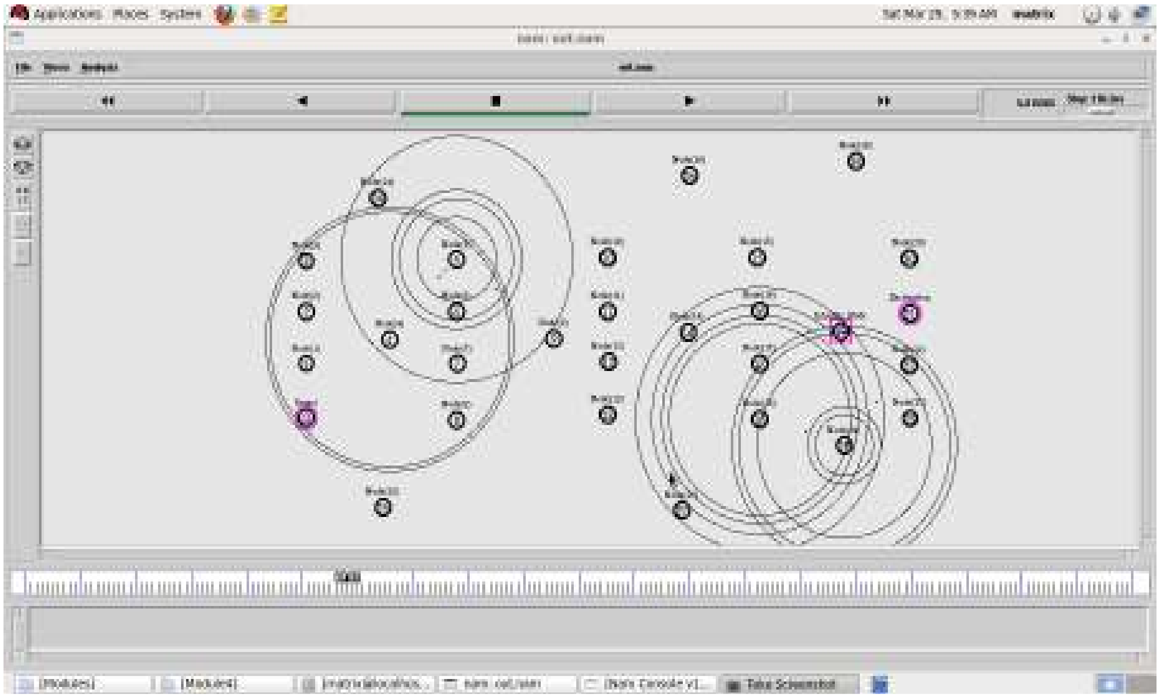

Fig. 9: Through redirection packet reached at destination

redirect the route from source to the destination. This will be reflected in the Fig. 8 and 9.

RESULTS AND DISCUSSION

Compare DAIHAODV with AODV and AIHAODV: In the previous chapter discuss the implementation of DAIHAODV protocol. This protocol implementation was based on the AODV protocol design principles. We made a performance comparison with AODV and AIHAODV protocol. Three performance measures we have taken are throughput, packet delivery ratio, End to End delay.

Through put between AODV and AIHAODV with DAIHAODV: Throughput refers to how much data can

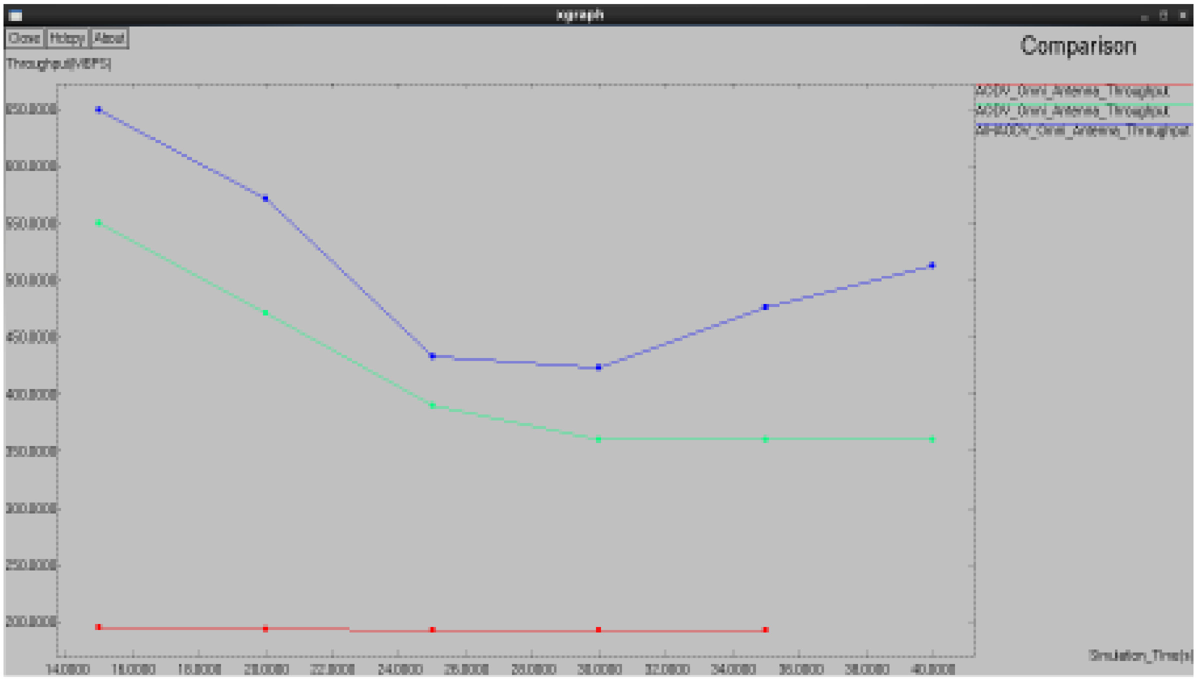

Fig. 10: Graph for throughput evaluation

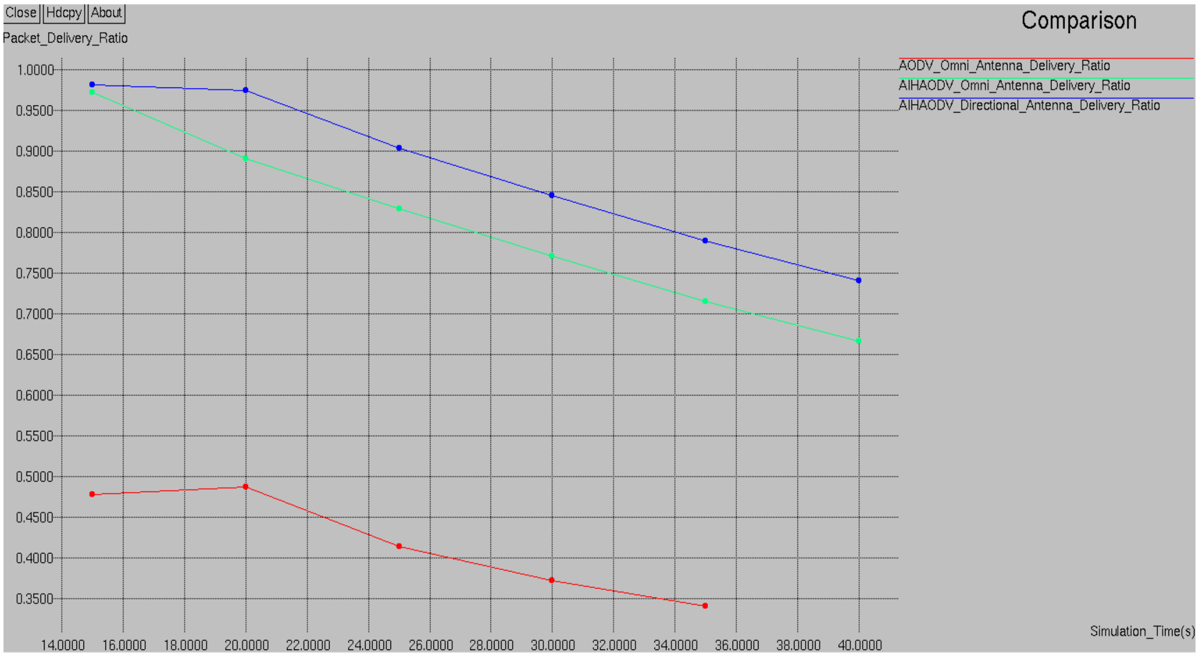

Fig. 11: Graph for packet delivery ratio

be transferred from one location to another in a given amount of time. Figure 10 shows that DAIHAODV protocol gets a better through put comparing with AIHAODV and AODV.

Packet delivery ratio: The ratio of the number of delivered data packets to the destination. This illustrates the level of delivered data to the destination:

$\sum$ Number of packets receive/$\sum$ Number of packets send

Figure 11 shows that DAIHAODV protocol gets a better packet delivery ratio comparing with AIHAODV and AODV.

End-end delay: The average time is taken by a data packet to arrive in the destination. It also includes the

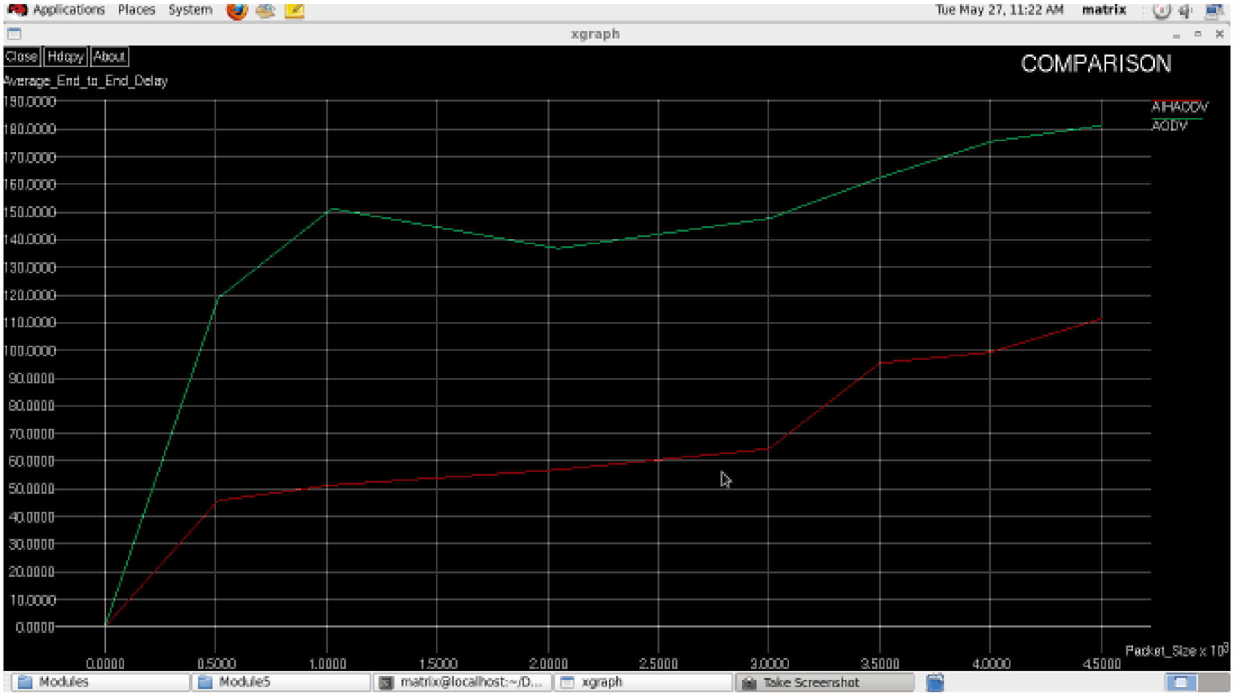

Fig. 12: End 2 end delay

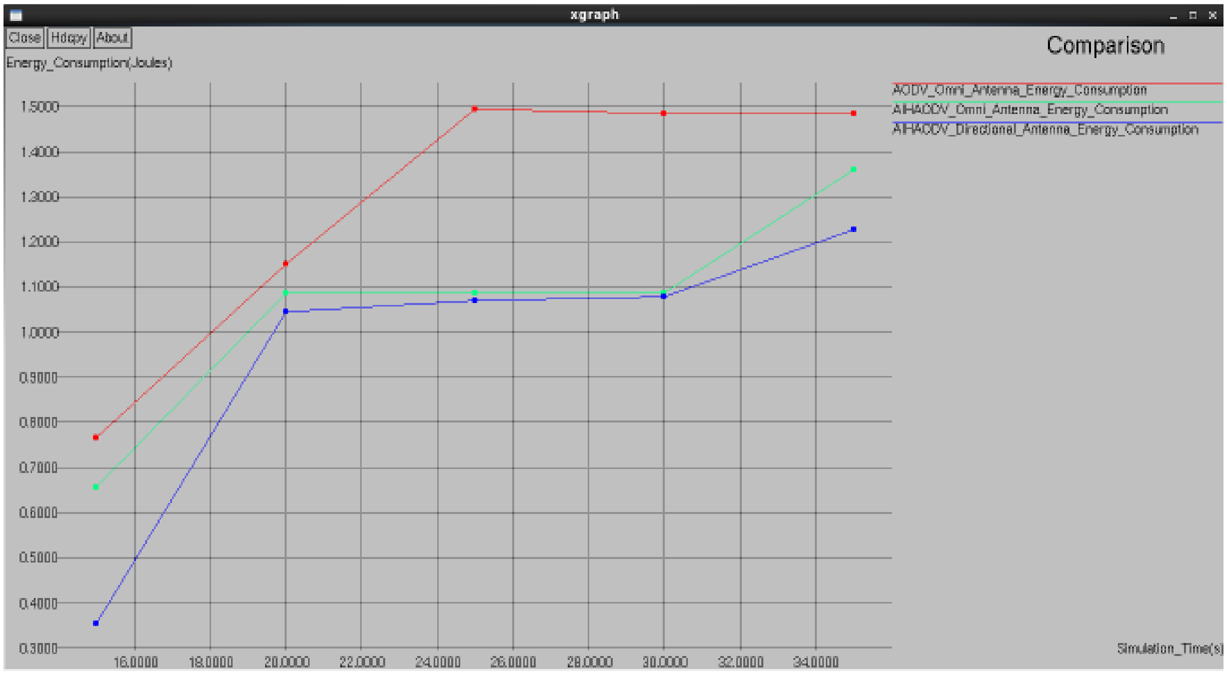

Fig. 13: Energy consumption

delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted:

∑ (arrive time-send time) /∑ Number of connections

Figure 12 shows that DAIHAODV protocol gets a better end to End delay comparing with AIHAODV and AODV.

Energy consumption: Figure 13 shows that DAIHAODV protocol gets a better energy consumption with AIHAODV and AODV.

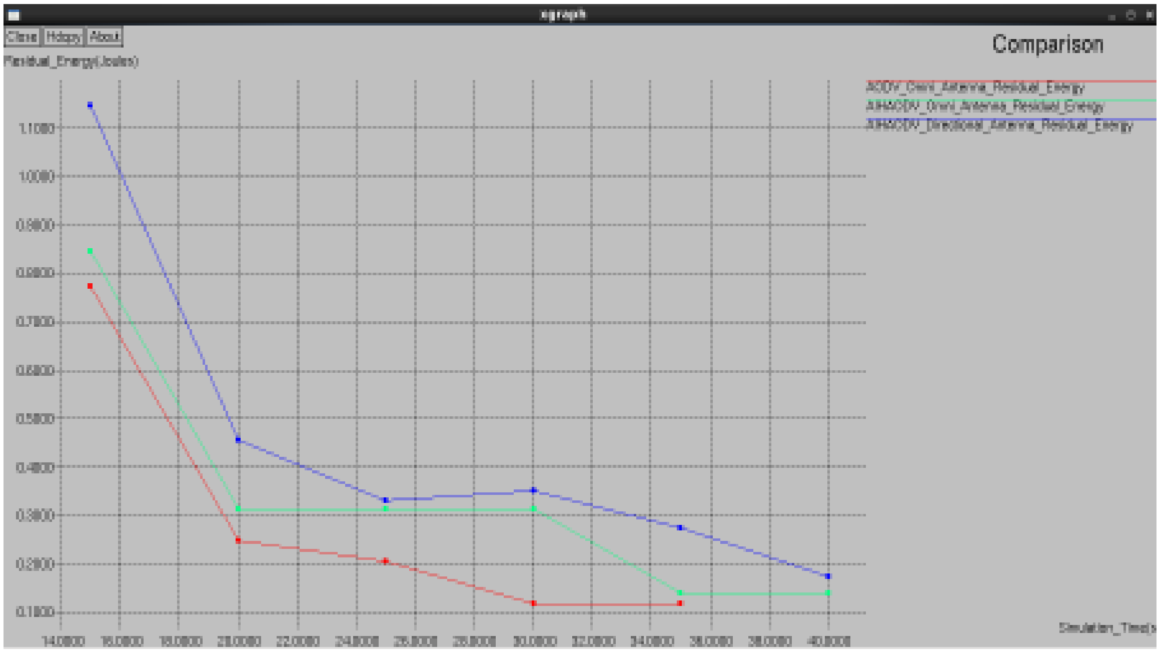

Fig. 14: Residual energy comparison

Residual energy: Figure 14 shows that DAIHAODV protocol gets a better residual energy comparing with AIHAODV and AODV.

CONCLUSION

This study presents, the implementation of Advanced DAIHAODV protocols using the divide and conquer strategy, was developed for identify victim node, intruder detection and power consumption using directional antenna. The performance factors energy level are compared with AIHAODV and AODV protocol which proved better result. In future this protocol can be enhanced with developing of dynamic antennas used for packet transmission which can support the more flexible of packet delivery in mobility on nodes.

REFERENCES

Abd Rahman, A.H. and Z.A. Zukarnain, 2009. Performance comparison of AODV, DSDV and I-DSDV routing protocols in mobile ad hoc networks. Eur. J. Sci. Res., 31(4): 556-576.

Bace, R.G., 1998. An Introduction to Intrusion Detection and Assessment. Infidel Inc., ICSA Incorporation.

Bace, R.G., 2000. Intrusion Detection. MacMillan Technical Publishing, ISBN: 1-57870-185-6.

Bellur, B., R.G. Ogier and F.L. Templin, 2001. Topology broadcast based on reverse-path forwarding (TBRPF). IETF Internet Draft, Retrieved from: draftietf-manet-tbrpf-01.txt.

Chiang, C.C., H.K. Wu, W. Liu and M. Gerla, 1997. Routing in clustered multihop mobile wireless networks with fading channel. Proceedings of the IEEE SICON-97, pp: 197-211.

Dorothy, E.D., 1987. An intrusion-detection model. IEEE T. Softw. Eng., 13(7): 222- 232.

Giannoulis, S., C. Antonopoulos, E. Topalis and S. Koubias, 2007. ZRP versus DSR and TORA: A comprehensive survey on ZRP performance. IEEE T. Ind. Inform., 3(1): 63-72.

Jacquet, P., P. Muhlethaler and A. Qayyum, 1998. Optimized Link State Routing Protocol. Internet Draft, Retrieved from: draft-ietf-manetolsr-00.txt.

Johnson, D.B. and D.A. Maltz, 1996. Dynamic Source Routing in Ad Hoc Wireless Networks. In: Imielinski, T. and H. Korth (Eds.), Mobile Computing. Kluwer Academic Publishers, Dordrecht, pp: 153-181.

Kuosmanen, P., 2002. Classification of ad hoc routing protocols. Comput. Sci., 3(8): 574-582.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehaviour in mobile ad hoc networks. Proceeding od the ACM/IEEE International Conference on Mobile Computing and Networking, pp: 255-265.

Mukherjee, B., T.L. Heberlein and K.N. Levitt, 1994. Network intrusion detection. IEEE Network, 8(3): 26-41.

Murthy, S. and J.J. Garcia-Luna-Aceves, 1996. An efficient routing protocol for wireless networks. Mobile Netw. Appl., 1(2): 183-197.

Park, V.D. and M.S. Corson, 1997. A highly adaptive distributed routing algorithm for mobile wireless networks. Proceedings of the INFOCOM-97, 3: 1405-1413.

Park, V. and S. Corson, 1998. Temporally Ordered Routing Algorithm (TORA) Version 1. Functional Specification. IETF Internet Draft,Retrieved from: http://www.ietf.org/internet-drafts/draft-ietf-manet-tora-spec-01.txt1998.

Perkins, C.E. and P. Bhagwat, 1994. Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers. Computer Communications Review, pp: 234-244.

Perkins, C.E. and E.M. Royer, 1999. Ad Hoc on Demand Distance Vector (AODV) routing. Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA’99), New Orleans, LA, pp: 90-100.

Perkins, C. and E. Royer, 2000. Ad Hoc on Demand Distance Vector (AODV) Routing. Internet Draft, MANET Working Group, Retrieved from: draft-ietf-manetaodv-05.txt.

Perkins, C., E.B. Royer and S. Das, 2003. Ad hoc On Demand Distance Vector (AODV) Routing. Internet Draft. RFC 3561, IETF Network Working Group.

Stojmenovic, I. and J. Wu, 2003. Broadcasting and Activity-Scheduling in Ad Hoc Networks. In: Basagni, S., M. Conti, S. Giordano and I. Stojmenovic (Eds.), Ad Hoc Networking. IEEE Press, Wiley, New York.

Wikipedia, 2004. The Free Encyclopedia. Retrieved from: http://en.wikipedia.org/wiki/Mobile_ad-hoc_network (Accessed on: October 2004).

Yongguang, Z. and L. Wenke, 2000. Intrusion detection in wireless ad-hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom’2000), Boston, Massachussetts, pp: 6-11.